BFFDoom Technical Whitepaper

12-09-2017

Abstract

This Whitepaper was authored as a base document for "BFFDoom", detailing the features, functionality and research behind the new anonymous Cryptocurrency, as well as providing insight into its usage and implementation. Our Solution is based off of the CryptoNote code base platform, and incorporates multi-signature outputs and encrypted ring signatures.

The BFFDoom Project is based on CryptoNote technology.
(https://cryptonote.org/)

Table of Contents

Introduction

BFFDoom is a Crytpocurrency that will be developed by The BFFDoom Team aimed at bringing numerous benefits and financial freedom to its users one its own, and by contributing to BFFDoom by providing a stable currency for the expansive, dynamic, and integrated network that is BFFDoom. BFFDoom is Blockchain based, open-source Technology, and is publicly available to anyone at any given time.

Using BFFDoom is:

- **Fast**: With transactions occurring instantaneously, removing the need to wait for Bank transfers to be confirmed or sent through. Payment is as instant and final as touching a button.

- **Safe**: Apart from being a Cryptographically secured payment method on the forefront of security, users will now no longer have to divulge any payment information to third parties along the lines of Banking Details.

- **Reliable**: BFFDoom will be able to be transacted 24/7 with no exceptions, fully reliable not only transactionally but integrally.

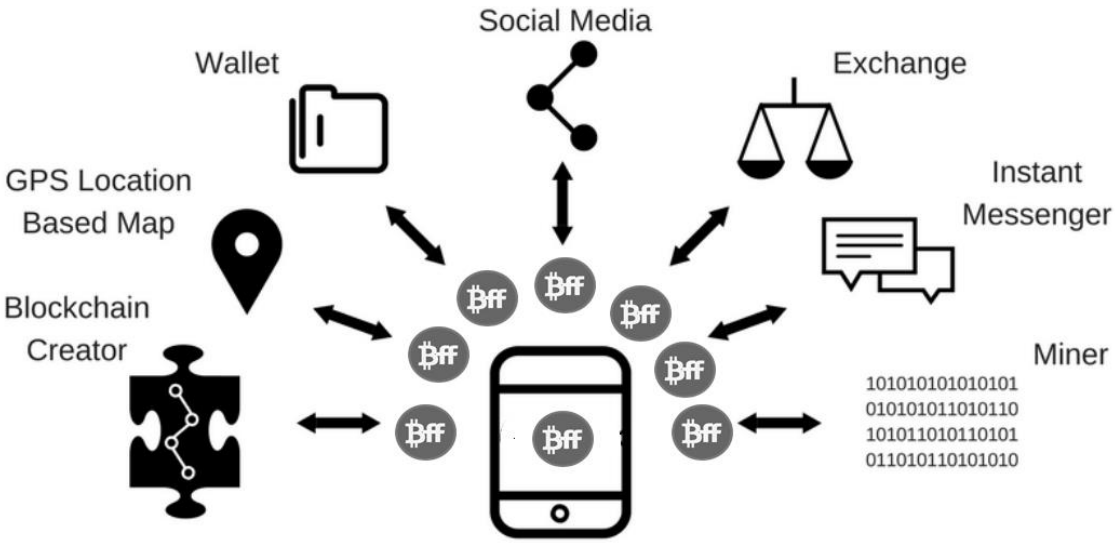
- **Convenient**: The use of BFFDoom will be fully user-friendly on all levels making sending or receiving payment less of a hassle and more of a pleasure.

Get ready to explore BFFDoom: The Cryptocurrency with a purpose

1- BFFDooms' Usage

A Cryptocurrency gets its value from how and where it can be used. By creating and identifying possible uses for BFFDoom we've ensured its value.

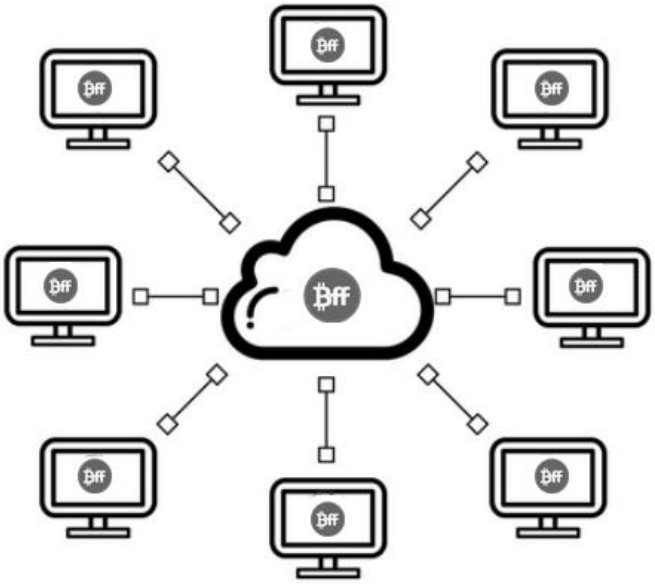
1.1- As the Base Currency of the BFFDoom App



BFFDoom will be the base and encouraged currency for use within the BFFDoom App.

All purchases and micro-purchases made from the BFFDoom App will be made using BFFDoom, this streamlines the process and makes the currency uniform for all features and functions of the App.

1.2- As Incentive for 3rd Party Miners

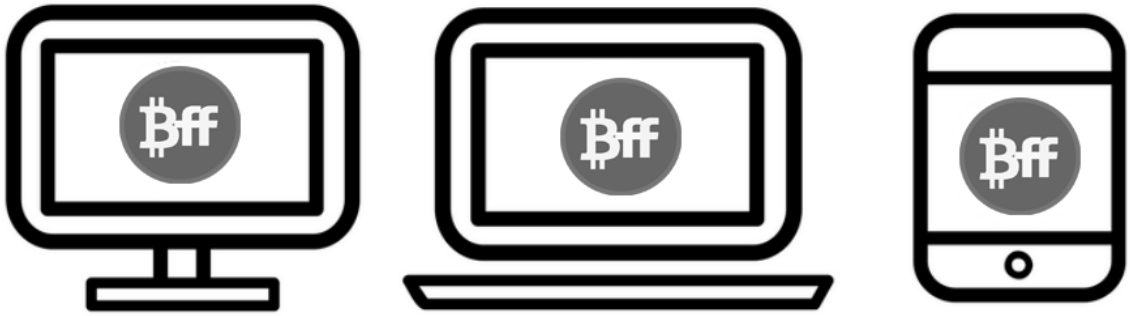


Every aspect and feature of the BFFDoom App is Blockchain based and therefore needs to be mined.

BFFDoom will be used to incentivise and encourage external miners to use their hashing power to maintain and speed up the BFFDoom Decentralized network.

Miners will not only be getting well compensated for their efforts, but are also making an active investment in themselves and the value of BFFDoom as a fast, functional Network will ensure a steady userbase creating usage and therefore value for BFFDoom.

1.3- As a Regular Cryptocurrency

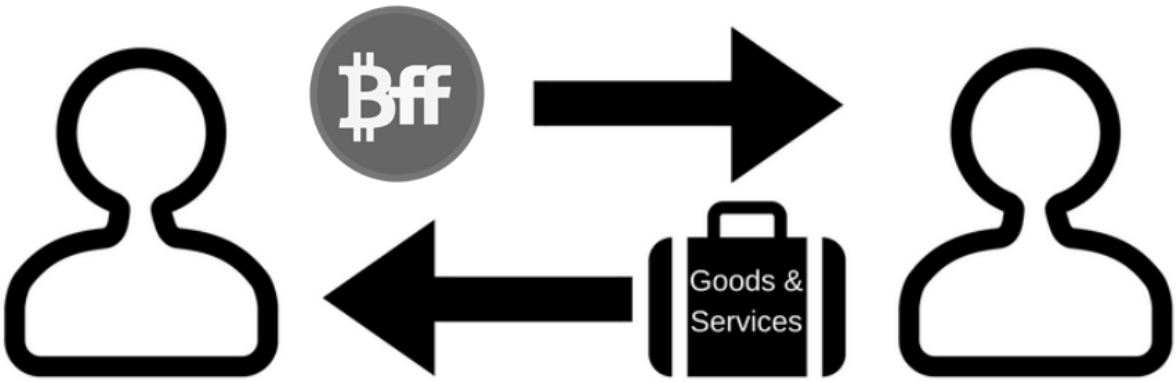


BFFDoom can be used just like any Cryptocurrency, and the usage of which is not bound to the BFFDoom app exclusively.

Users are encouraged to use BFFDoom across multiple platforms and even develop their own external frameworks, platforms, and applications implementing BFFDoom. Any Users wanting to do this will receive the full support, encouragement, and guidance of the BFFDoom team.

Take everything away and BFFDoom is an anonymous, functional, and value orientated Cryptocurrency that should be used on every level.

1.4- As a User to User Alternative for Cash

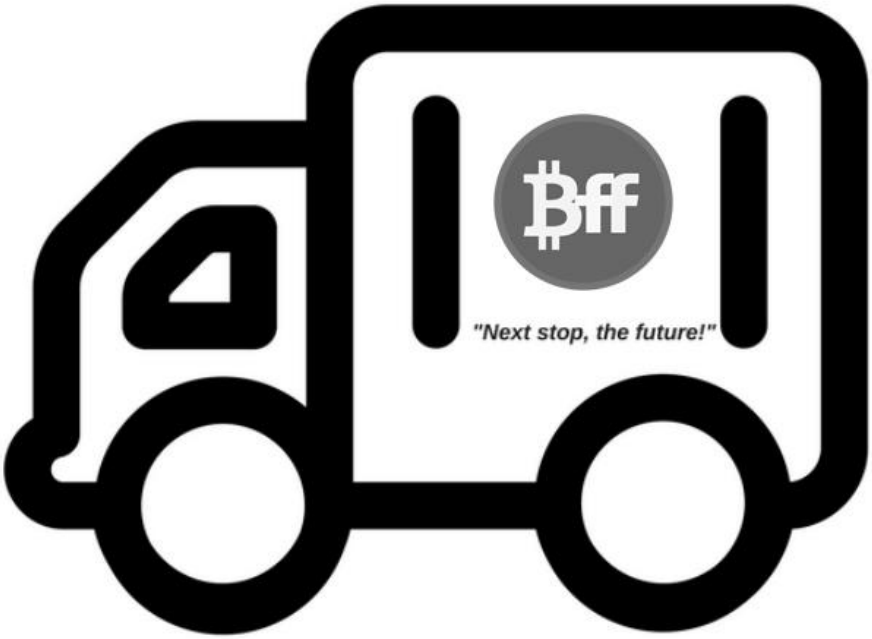


BFFDoom will foster the trading and exchange of Cryptocurrency for Goods and services on a User to User level.

Users are encouraged to shed the risks of using Fiat Currency between each other and instead use BFFDoom as they ensure safety and value on every level.

BFFDoom transactions will be conducted on multiple levels of use from large corporations to small businesses, to individual users. Its the directive of the BFFDoom Team to make sure that no area of use is neglected and BFFDoom use is fostered on all levels of use.

1.5- As a Long-Term Investment Vehicle



BFFDoom is the fundamental opposite of Fiat currency when it comes to the storage of value.

Users can easily make long-term investments with large returns as BFFDoom is anti-inflatory and gains value over time. Dynamic Block sizes scalable difficulty and steady rewards mean that BFFDoom will be built on value, and the increase thereof.

So whether you're purposefully saving an investment holding of BFFDoom or not, the price and value of BFFDoom is guaranteed to rise overtime by design creating many a millionaire along the way, will you be one of them?

1.6- As a Daily Usage Currency

BFFDoom were designed for use on a daily level.

The infrastructure of the BFFDoom App allows for simple hassle free usage of BFFDoom daily.

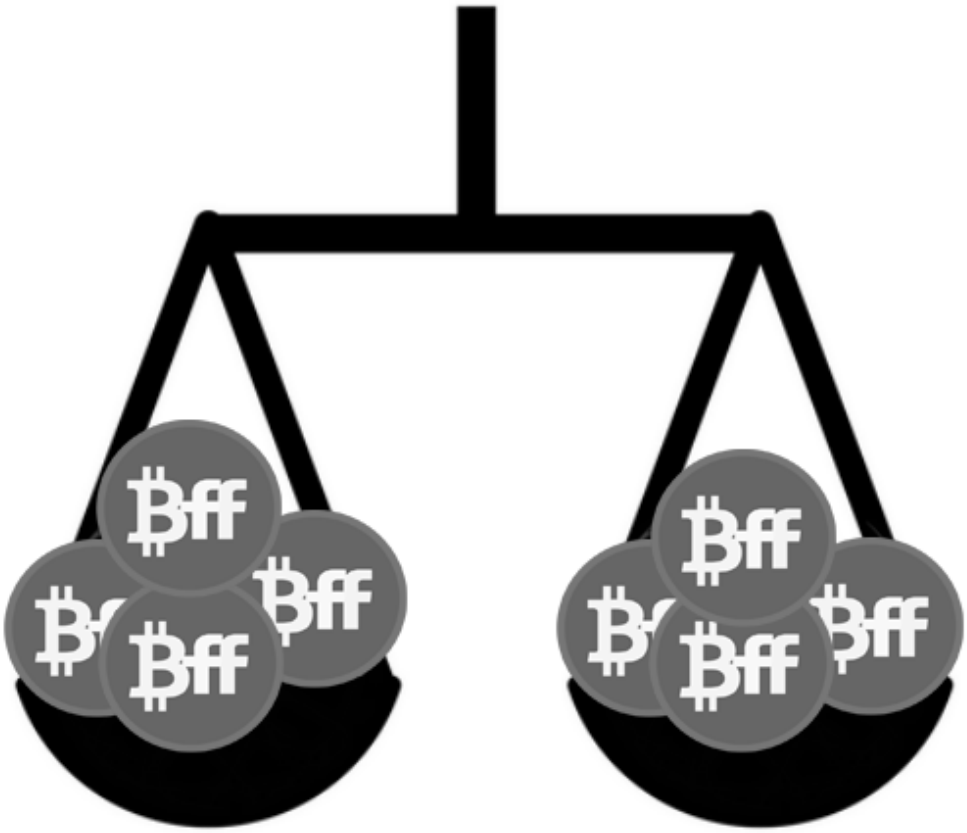
The BFFDoom Wallet-Linked Debit Card makes BFFDoom payment even easier by letting you pay with BFFDoom wherever a card payment point is available.

As the list of Businesses registered with BFFDoom grows larger over time Users will be able to spend their BFFDoom directly at a range of Businesses and store making BFFDoom a truly usage centric Cryptocurrency.

2- BFFDoom' Features

BFFDoom is a feature rich Cryptocurrency that can function on its own, even without the support and infrastructure of the BFFDoom App.

2.1- Fungibilty



Fungibility is a property that can be defined as “Inter-changable Value” for example a dollar is interchangeable with another dollar and therefore is fungible.

Bitcoin and other Cryptocurrencies that have transparent Blockchains however are not fungible. This is due to the fact that any Coin with enough effort can be

traced back to it's origin and in fact there are many agencies and organizations that primarily do exactly that.

Bitcoins are often blacklisted by certain organizations and not accepted as payment due to their previous use in illicit activities among other reasons. But if you aren't engaging in illicit activities there's no need to worry right?
Wrong, any coins you receive could have been used in illicit activities further down the Blockchain potentially creating complications for you.

Imagine you're at the grocery store and the clerk tells you that you can't pay for your groceries using your $100 Bill because it was used to buy drugs 3 years ago, doesn't seem reasonable does it?

That's why it has been concluded that any Cryptocurrency with a transparent Blockchain is not fully fungible, due to the long history attached to every coin, one Bitcoin simply does not equal another.

We've ensured that all BFFDoom are totally fungible and free of any influencing factors that could lead to any form of "Blocking", "Flagging", or otherwise denial of use.

2.2- Security

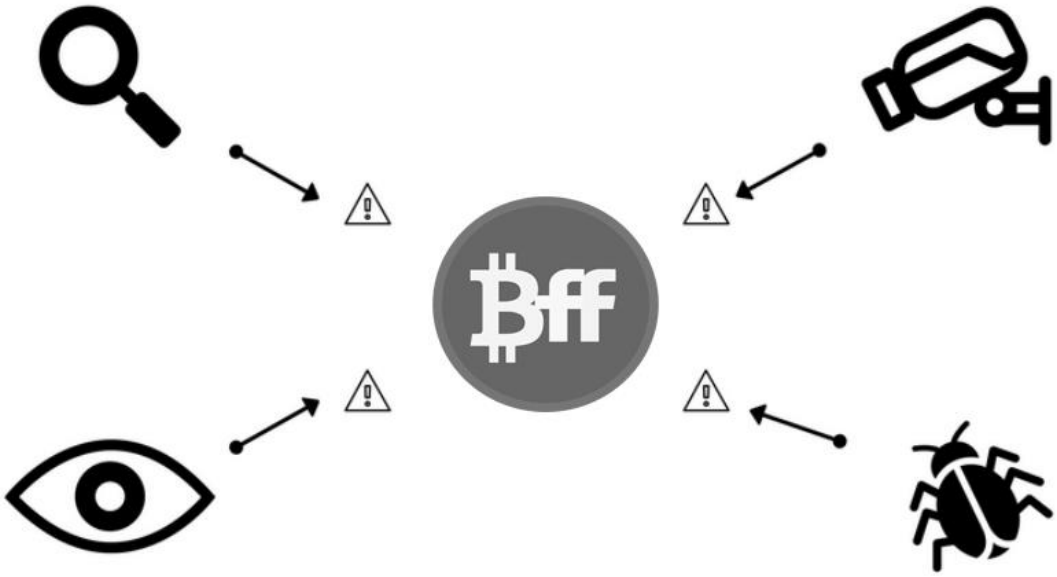
Security has been a hot topic of discussion when it comes to Cryptocurrencies for a long time. The security of many Cryptocurrencies is being called into question due to the inherent dangers of the online world such as hacking attacks and data breaches.

The BFFDoom team has put our minds together and formed a security policy to prevent, deter, and eliminate the threat of external malicious attacks on our system.

We’re all about dynamic security, there’s no such thing as a 100% impenetrable system however we’re doing our best to come awfully close with planned regular security updates and enhanced security measures.

Cryptocurrencies as a whole are on the forefront of online security and encryption. Cryptography is quite literally the study of secure communication and encryption. When it comes to the safety and security of our users we take no short cuts, keeping our user’s private information private is one of our top priorities, and we’ve got the technology to make this possible.

2.3- Privacy



Privacy is without a doubt one of the most important features of any Cryptocurrency.

Bitcoin and other Cryptocurrencies with transparent Blockchains are generally perceived to be anonymous when in actual fact they are pseudo-anonymous.

We touched on earlier how transparent Blockchains detract from the fungible value of a coin, but they also pose a serious privacy risk too.

Using a pseudonym to conduct Bitcoin transactions is much like wearing a balaclava in public, while you might be hiding your identity in the short term, anyone following you and seeing what stores you go to, who pays you money, and who you give money to will soon be able to piece together who exactly you are.

The only difference here is that using Bitcoin all this information is public and accessible at any time online, no one has to actually follow you around.

When you use BFFDoom, dynamic ring signatures and our analysis resistant Blockchain render you 100% anonymous allowing you to immerse yourself in complete privacy, and you can breathe easy knowing that while conducting your business, your information is inaccessible to prying eyes.

2.4- Feasibility

One of the core elements incorporated in designing BFFDoom was feasibility and overall practical use.

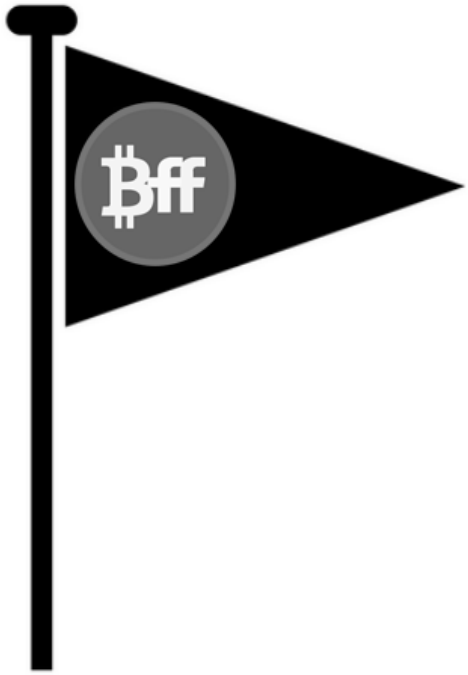
We want BFFDoom to be a beacon of success in the Cryptocurrency world and we're of the belief that all our users, big and small, are entitled to a share in the prosperity.

The BFFDoom App is a cornucopia of feasible features and usage for BFFDoom and as such will create a steady userbase that will guarantee the value of BFFDoom

To make this possible we've made sure that using BFFDoom makes not only practical sense, but Financial sense as well. It's well known that Mining is the most profitable Cryptocurrency activity, however for many pseudo-annoymous coins this is fast becoming untrue.

However mining BFFDoom is not only easy, affordable, and fair due to our egalitarian proof of work algorithm. But it’s also private, when you mine BFFDoom you are truly mining a Cryptocurrency in every sense of the word, your identity and how much you mine are kept totally enigmatic from start to finish.

2.5- Sustainability



“Slow and steady wins the race” The tortoise said to the hare. BFFDoom hasn’t strayed far from this ancient proverb.

While BFFDoom are all about profit we also keep the concept of sustainability close to heart.

There can be no shortcuts to getting BFFDoom to the level we ultimately desire. That’s why BFFDoom and the BFFDoom App were designed for the long run, incorporating measures to make sure that both can withstand the test of time, and build a large user base with a dynamic network that’s always adapting along with it’s users.

2.6- Speed

Speed is an often touched on point by many Cryptocurrencies, and rightfully so, having a fast network works wonders, especially in the complex world of Cryptocurrency.

Our team has devoted a good portion of our time to make sure that our Network is as fast as possible. From transaction speed to Wallet syncing we've optimized every angle to get it running as fast as it should, and it's an ongoing process!

The inclusion of External miners into the BFFDoom Network will provide a massive boost in speed and functionality for both BFFDoom and BFFDoom.

We're constantly devising new ways to save our users even more time and add to the convenience factor of our currency. Nothing is more frustrating than waiting hours for a Transaction to be processed or a function to work.

To us, speed isn't a luxury, it's a necessity. After all, Time is money!

3- BFFDooms' Technology

BFFDoom incorporate CryptoNote Technology which is Ground-Breaking in the Field of Cryptocurrencies and provides a unique set of features and benefits other Cryptocurrencies simply don’t have.

3.1- Untraceable payments

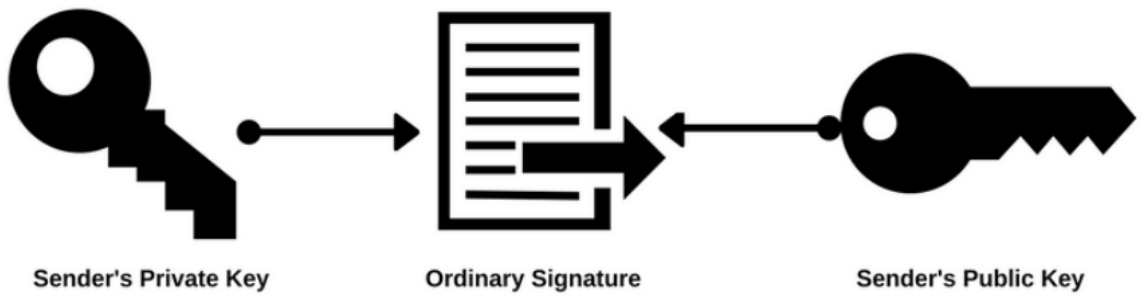


Figure 1: Ordinary Cryptocurrency signature

Generic Cryptocurrency verification processes include using the public key of the transaction signer, this is needed because it proves that the signer is in possession of the private key that matches his public key. However this generic verification process creates a large security gap.

BFFDoom employ Ring Signature technology. The Ring signature verification method makes use of multiple different public keys during one verification in a group of people, still each with their own public and private keys.

The main difference here being that looking from an external perspective it's impossible to determine who within the group is actually requesting the transaction.

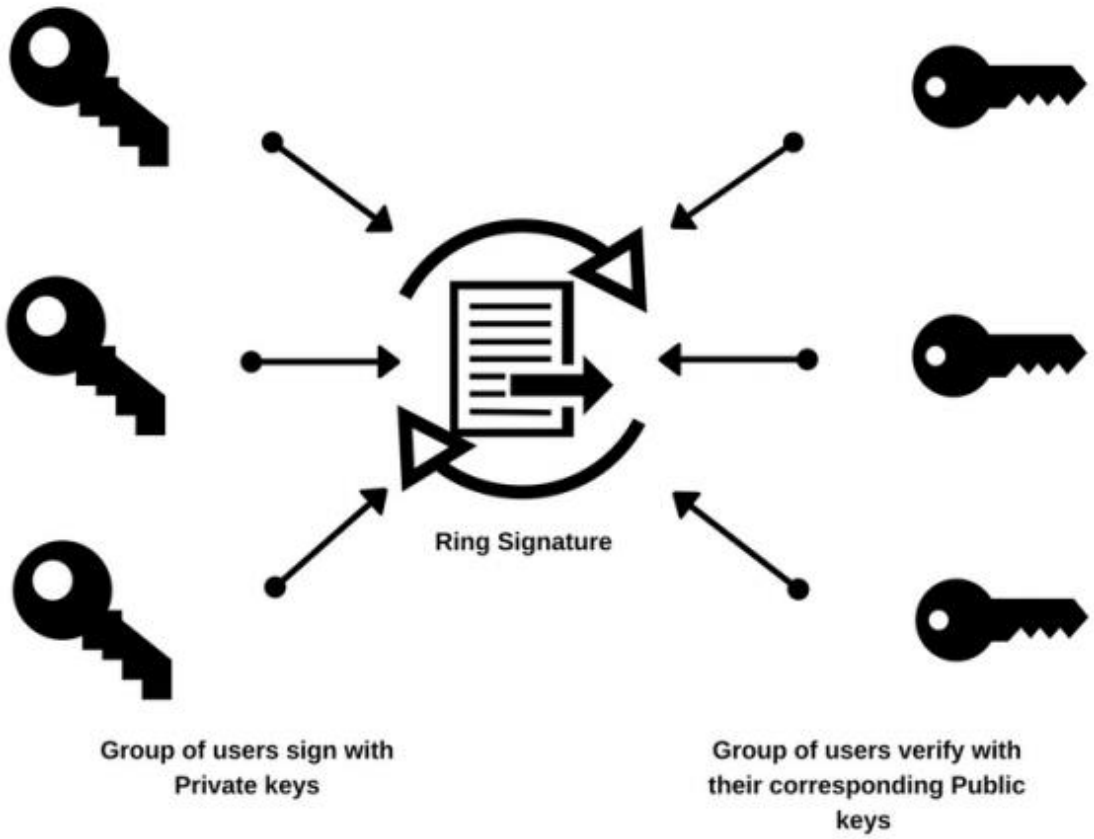


Figure 2: Ring Signature

Using this concept to send BFFDoom transactions ensures users that:

• A- Transaction creators are eligible to spend the correct amount
• B- Transaction creators' identities are indistinguishable from the other users' public keys used to make the Ring signature.

Ring signatures combine functionality with privacy seamlessly.

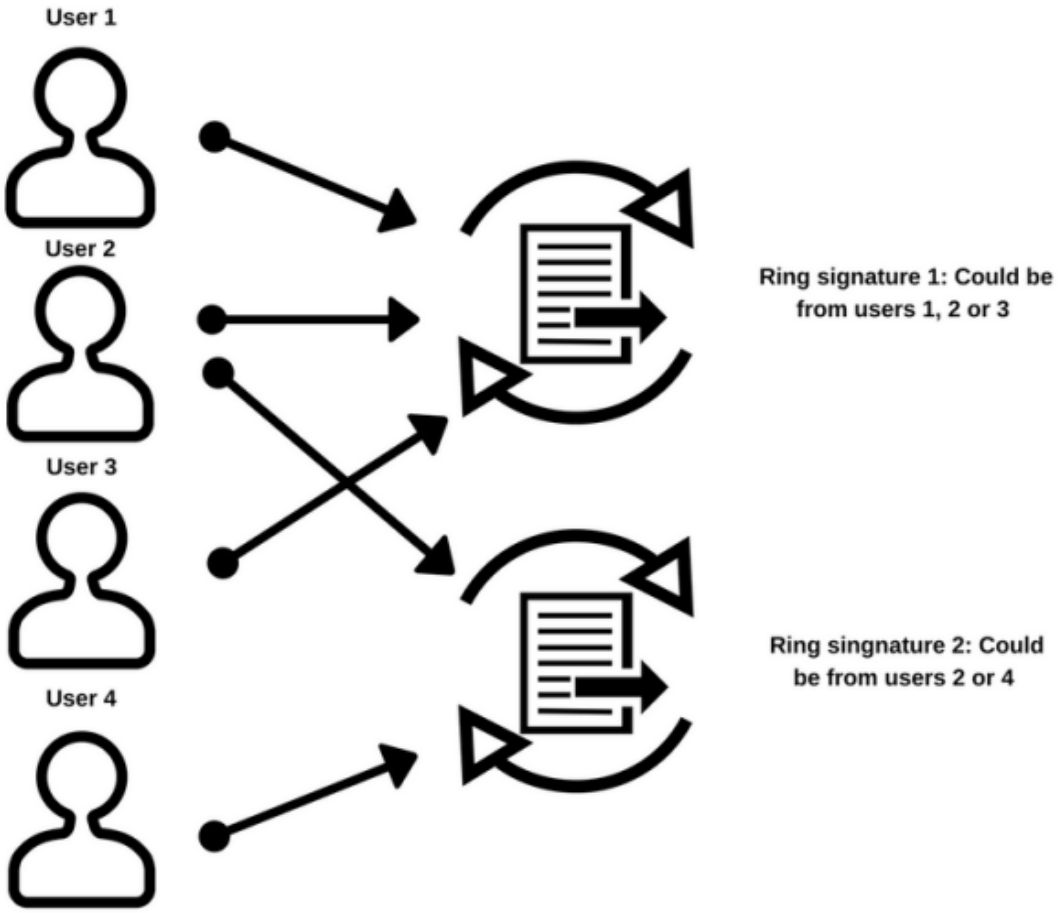


Figure 3: Ring Signature ambiguity

It's worth mentioning that even though your public key will appear in many Ring signatures that you didn't request hiding other users' identity, it will in no way affect you, or your ability to Send/Receive BFFDoom.

3.2- Double spending proof

100% Anonymous Ring signatures would let users spend the same funds over and over again without consequence, logically this can't work with any financial system.

BFFDoom fixes this problem by employing a modified traceable ring signature system with a built in feature to restrict Double-spend attacks that are common in other Cryptocurrencies.

If a malicious user attempts to create more than one ring signature using the same private key, even if the public keys used are different, the signatures are then linked by the system and flagged as a double spending attempt.

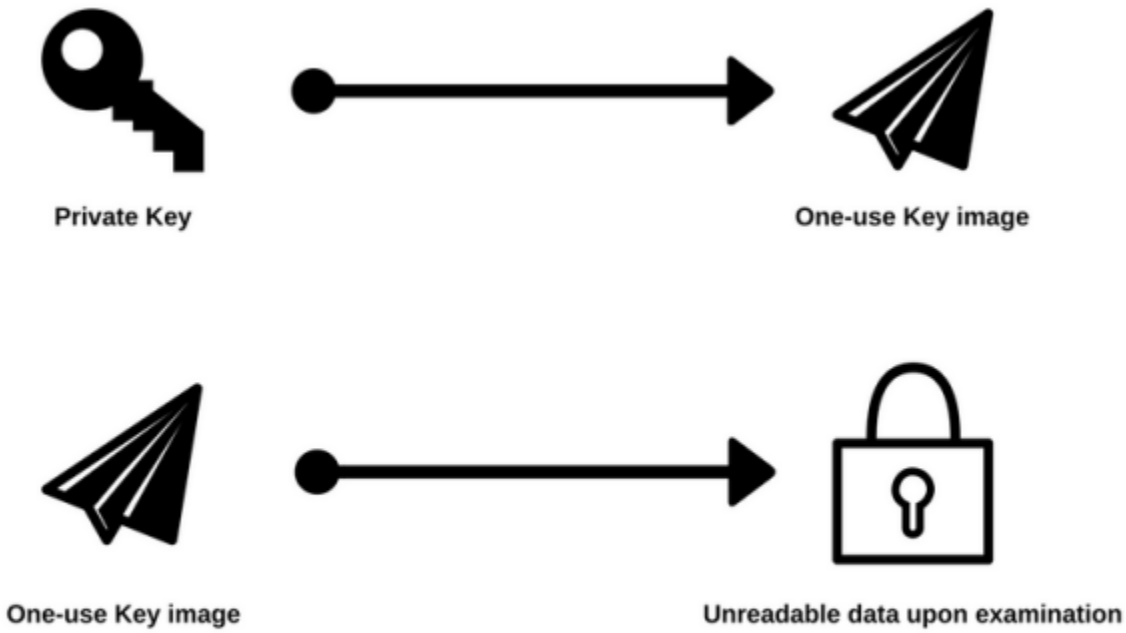


Figure 4: Key images

To do this we use "Key images", these are one-way cryptographic imprints of private key. No two Key images are going to be the same, exactly like no two private keys are going to be the same.

While key images stand as a measure to prevent double spending, they don't let anyone discover the private key they belong to.

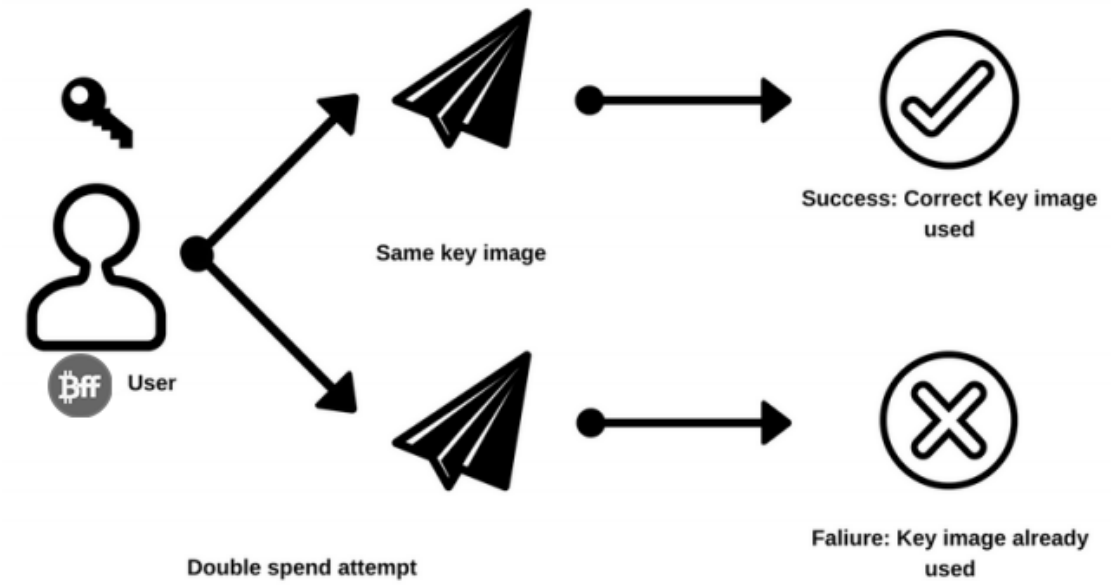


Figure 5: Double-spend Check

All BFFDoom users will have installed on their wallets an updated list of all currently used Key images, when you compare the file size to Bitcoin which requires you to download the entire Blockchain (Full record of all transactions), you'll find the Key image database size is much smaller and more convenient.

Using Key images is our way of preventing Double-spending, while also keeping our Users' identity safe. If you make committing the crime impossible you won't have to punish anyone.

3.3- Unlinkable Transactions

When using most Cryptocurrencies, any time you make use of your public address anyone can conduct blockchain analysis to determine your wallet balance by comparing data from your transactions. Even when you're protected by Ring signatures your incoming transactions can still be analysed. One can attempt to solve this problem by creating a new public address over and over again with every new transaction, but doing this would soon develop into a chore detracting severely from your convenience factor.

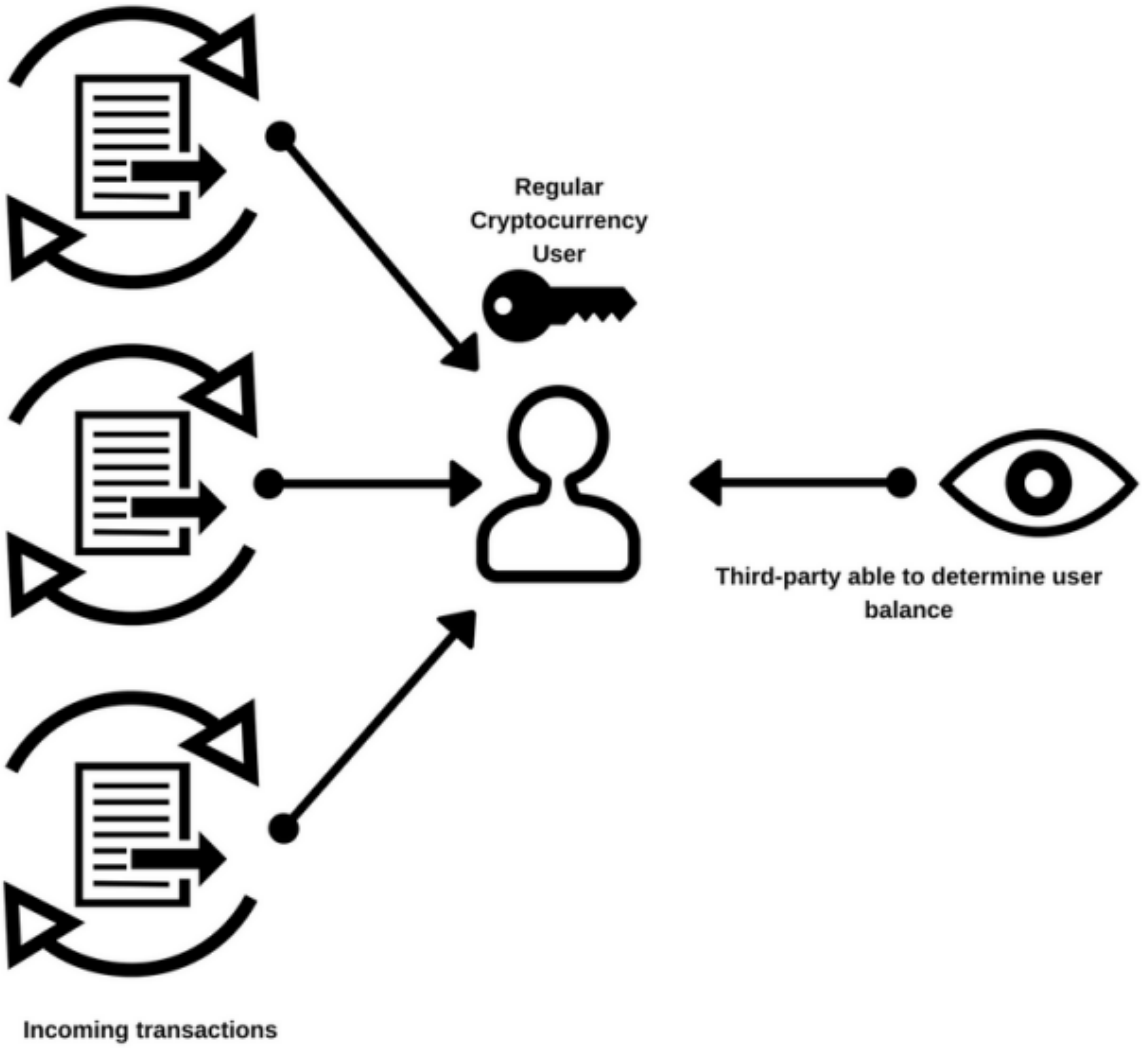


Figure 6: Linkable transactions

Our solution for our currency is to implement a system in which we automatically creates multiple one-time transaction keys derived from your public key for every transaction you conduct. This is possible by modifying the Diffie-Hellman exchange protocol which originally allows two users to produce a mutual secret key which is a derivative from their public keys. We use the receivers public key and random data generated by the sender to generate a unique one-use key to verify the payment.

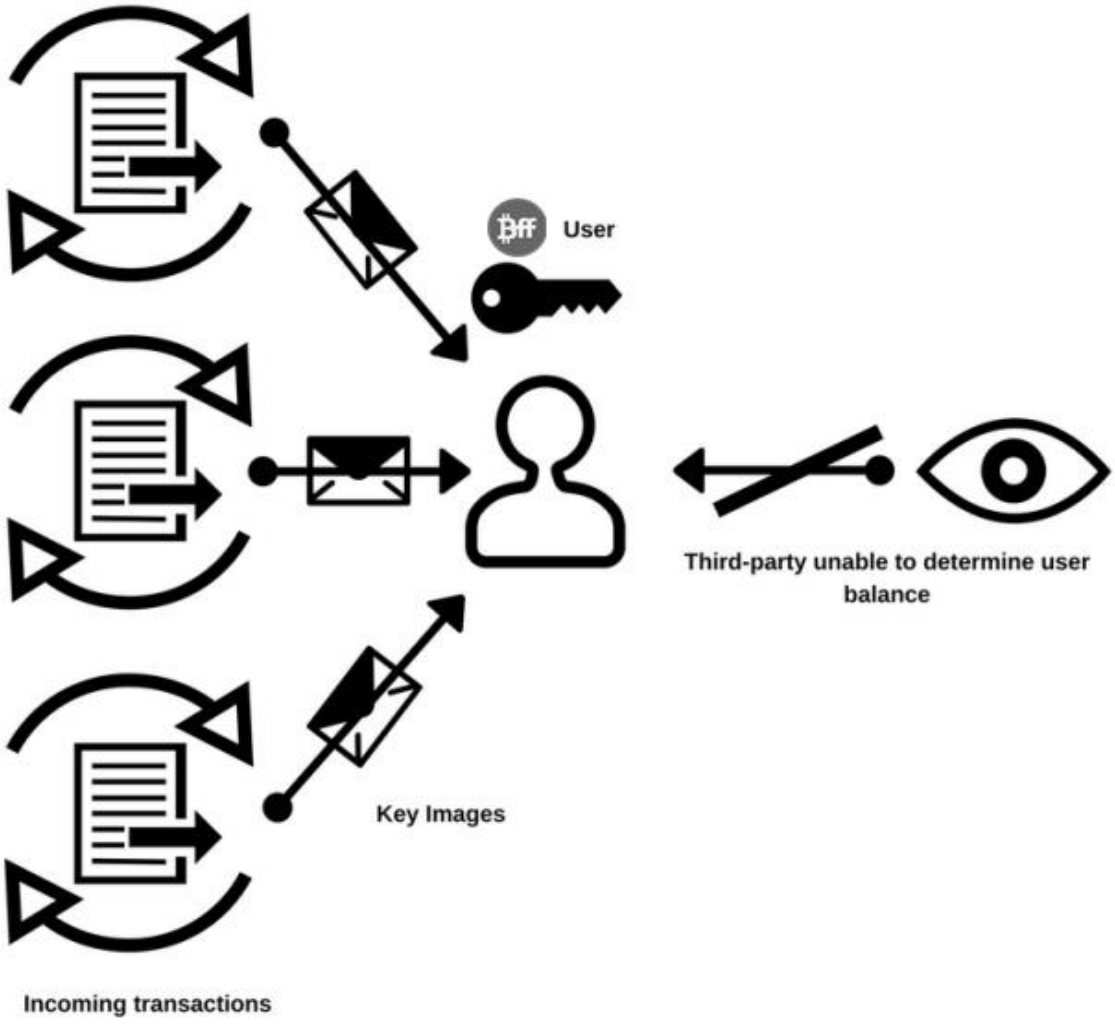


Figure 7: Unlinkable transactions

Senders can only generate the public part of their keys, while receivers can only read the private part. Therefore third-parties can't possibly analyse transactions as they are a strictly peer-to peer in the truest sense of the term.

3.4- Blockchain analysis resistance

It's possible for anyone, with enough time and resources on their hands, to fully trace any Bitcoin all the way back to when it was mined, finding out the exact path it went along the way, often leading people to conclude who owns what, who sent what, and sometimes who people are.

This is attributed to Bitcoin's transparent blockchain, due to it's nature, every transaction has unique variables that are all traceable.

What makes tracing these transactions even easier is users reusing the same addresses multiple times (Even though Satoshi recommended using a different wallet address for each transaction, not that it actually helps much.)

The BFFDoom team makes a much different approach, our system is designed to eliminate the risks involved with key re-usage, and traceable variables. We learned earlier that Ring signatures are derived from a mixture of sender and receiver data, by doing this we provide an anonymous, private, secure platform for our users.

By their very nature Ring signatures are anti-analytical, depending on the size of the signature, the analyst could be trying to determine the original sender in a group of anywhere from 2-1000 people, with every new transaction added to the list making tracking coin paths an increasing impossibility.

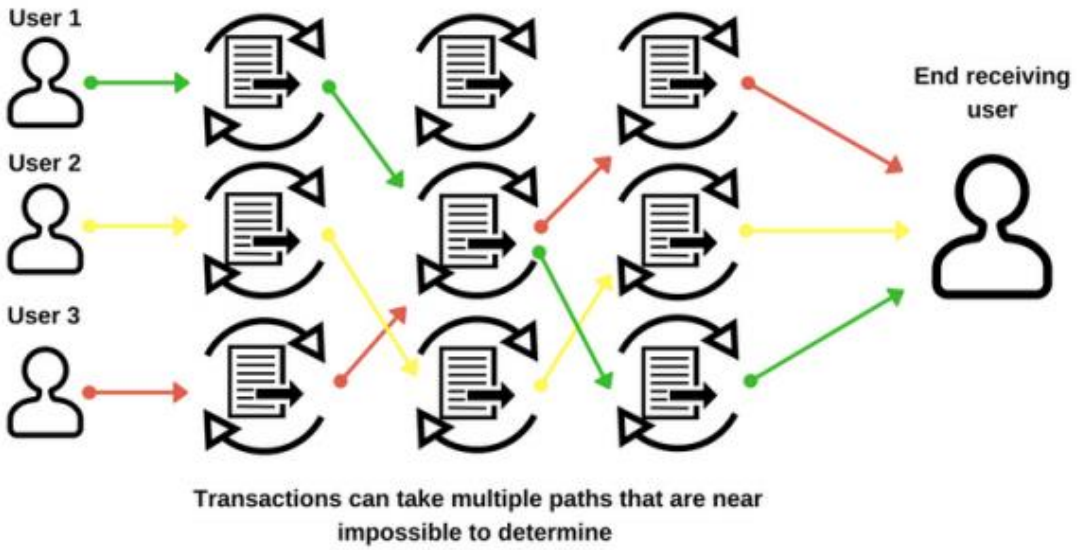


Figure 8: Blockchain ambiguity

3.5- Egalitarian proof of work

BFFDoom’ proof of work system is a true rendition of Satoshi's famous phrase "One CPU - One Vote" Our users have the right to vote on New features, transaction order, and supply distribution.

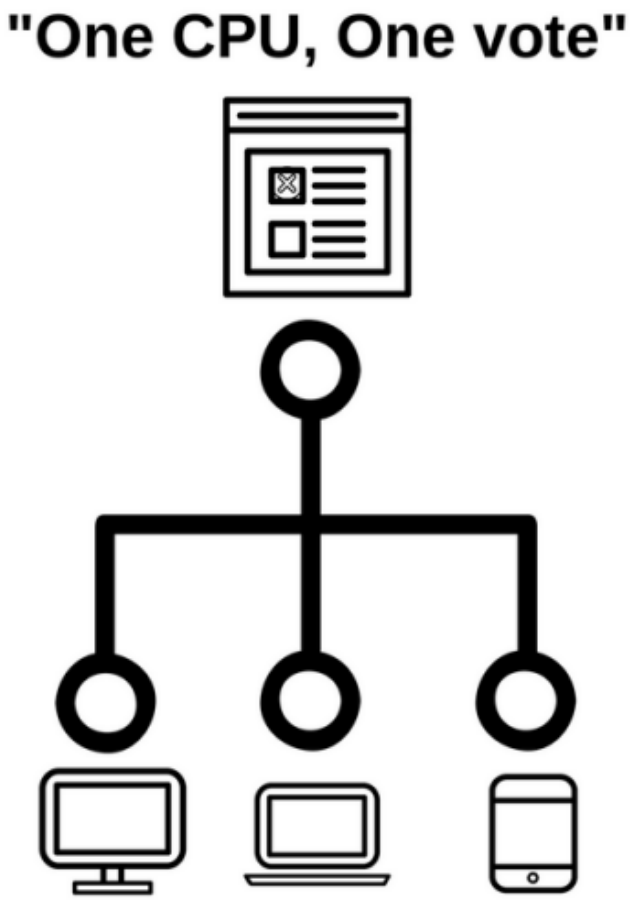


Figure 9: One CPU, One Vote

A Key part of the democratic system is each vote holding the same power. That's why we made sure that all users have equal voting rights.

We employ an Egalitarian proof of work function that is perfectly suited for a multitude of devices.

Our scripts are designed to be complex and lightweight, perfect for a CPU to process, but way too difficult and expensive for advanced mining hardware like ASIC cards and dedicated mining hardware.

Our function depends on a slow stream of memory with an emphasis on latency dependence, every 64 byte long block directly depends on all previous blocks. The resulting effect is an exponential increase in calculation speed.

The algorithm requires only approximately 2 MB per instance, this is because it fits perfectly into the L3 cache present in every core of modern processors, which have been in circulation for many years.

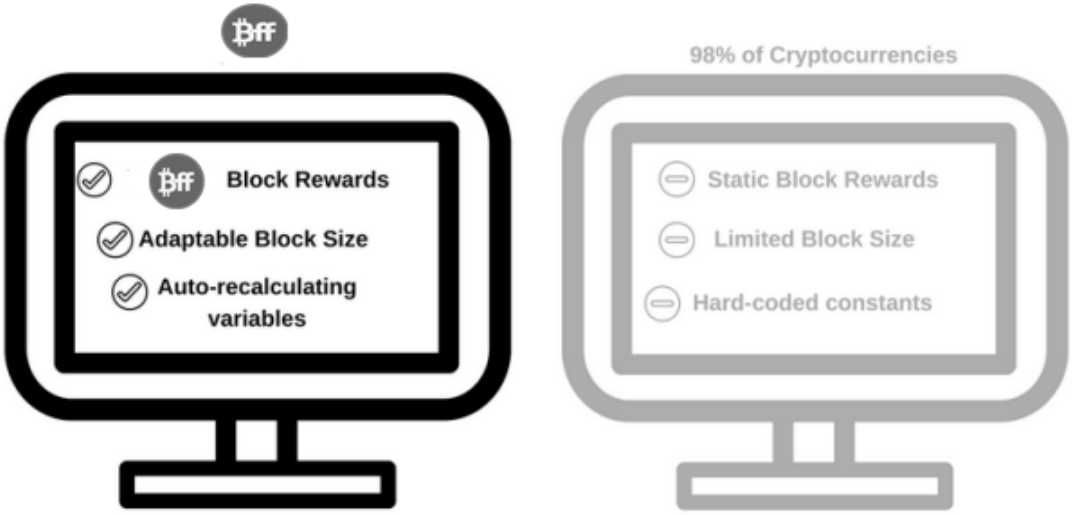
Also a megabyte of internal memory usage will render any ASIC card impractical for use. GPUs and ASICs can run hundreds of instances in parallel but are limited by GDDR5 memory which is infinity slower than an Average CPU's L3 cache.

3.6- Adaptive parameters

The BFFDoom team believes that for a currency to be viable, it must not depend on a single person, or a small group of peoples' decision (Someone tell the fiat currencies!).

Bulky Hard-coded constants and magic numbers present in the code of most Cryptocurrencies act as an inhibiting factor for their growth, stability, and overall functionality.

Our solution is to incorporate dynamic, auto-recalculating variables in place of these constants to provide a platform for a currency that improves alongside it's users.



Almost every crucial limit from Block size to Block Reward is fully adaptive and reactive. Each BFFDoom Block recalculates difficulty using an algorithm that adds the sum of the work done in the previous 720 blocks and divides it by the

amount of time used to solve them, while cutting off 20% of the outliers in the data set.

As for our Block size, we employ an algorithm that prevents a bloated inconsistent blockchain, but yet still doesn't apply a "Hard Limit" onto blocks, allowing for steady growth of blocksize overtime as the network grows and needs to meet the demands of more users.

Conclusion:

While many Cryptocurrencies exist on the market today, BFFDoom will stand out as a unique blend of feature and framework incorporating advanced CryptoNote Technology and being anchored by the expansive and dynamic BFFDoom App.

Looking over BFFDoom as a whole it's plain to see that we're equipped for success.

We've got the technology, human resources, and motive to mould the BFFDoom into a Cryptocurrency to rival all others.

- We've taken a brief look into BFFDoom' usability, how BFFDoom can and will be used across a multitude of platforms and for a plethora of different reasons.

- We've explored the base features of BFFDoom and the beliefs that hold it together at it's core and sets BFFDoom apart from the rest of the pack.

- And we've had an overview of the Technology that allows BFFDoom to deliver on all its features and functionalities.

By now I'm sure you agree that BFFDoom and BFFDoom together make a genuine recipe for success, in fact we've already started Cooking!

Special thanks to the CryptoNote team for making their technology open-source and adaptable to our BFFDoom' needs. We hope that you continue to grow and prosper.